The Information Commissioner's response to the Consultation on a new legal duty to support a multi-agency approach to preventing and tackling serious violence

The Information Commissioner is responsible for promoting and enforcing data protection law in the UK including the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). She is independent of government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. She does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken. She welcomes the opportunity to respond to this consultation.

Many of the consultation questions fall outside of the scope of the Information Commissioner's regulatory role as they are directed towards organisations with expertise in working with young people at risk of criminal involvement. For this reason, key data protection points are addressed below rather than using the questionnaire. Where possible, the question headings used in the consultation are maintained.

The Information Commissioner recognises the importance of preventing and tackling serious violence. The sharing of personal data can bring benefits to everyone: to society, to organisations, and to individuals. Data protection law provides a framework for controllers of personal data to apply appropriate safeguards to protect it. This is particularly important in this context, given its sensitivity and the potential for harm if there is inappropriate disclosure or loss.

It is important that when organisations share personal data, that it is compliant with data protection law, in ways that are fair, transparent and accountable.

Part 3

Q 8. Do you agree that the vision and focus for a multi-agency approach to preventing and tackling serious violence is correct? If not, please explain why?

The Information Commissioner recognises that a multi-agency approach can be an effective way of preventing and tackling serious violence. However there are data protection obligations that organisations must adhere to when conducting multi-agency data sharing. Particular attention must be given to the processing of sensitive personal information, and data protection law provides a mechanism for organisations to share data when necessary. It is important to recognise where models of existing good practice in data sharing exist and to build on these.

Our recent blog: 'Data Protection law does not prevent information sharing to save lives and stop crime' reminds organisations that the new data protection legislation does not stop the disclosure of personal data to assist police forces or other law enforcement authorities. It reinforces the message that data protection law should not be a barrier to sharing when it is necessary to protect the public.

Under the circumstances set out in the consultation, it is likely that there will be a requirement to conduct a Data Protection Impact Assessment (DPIA). Conducting a DPIA enables controllers to systematically analyse, identify and minimise the data protection risks of a project or plan, or where there are changes to existing processing. It is a key part of a controller's accountability obligations and demonstrates how they comply with their data protection responsibilities. In the context of this consultation, the DPIA should address how the processing in each of the proposed options would address the objectives set out in the government's Serious Violence Strategy. Detailed guidance on conducting DPIAs is available on the ICO website.

If there are to be changes in the legislative framework relating to data processing, then there are new obligations for government to consult with the Information Commissioner. Article 36 (4) of the GDPR sets out the requirement relating to prior consultation with the Information Commissioner, it states that:

Member states shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

Further engagement with the Information Commissioner at the outset would help ensure that compliance will be addressed at an early stage, which should support practitioners further down the line. We would welcome this engagement. Robust data protection measures will be necessary in supporting practitioners with any new data sharing obligations placed on them.

The Information Commissioner is currently updating her Data Sharing Code of Practice (the code) to reflect changes in data protection legislation; it will also explain new developments to take into consideration. We anticipate that the draft code will go out for public consultation over the summer; the Home Office may wish to engage with the ICO during this consultation period. The aim is for the code to be laid before Parliament and become statutory later in the year. Due regard should be given to the code when developing the multi-agency approach set out in this consultation.

The new code will, in accordance with section 121 of the DPA 2018, provide "practical guidance in relation to the sharing of personal data in accordance with the requirements of the data protection legislation". Adhering to the code will help to ensure good practice around data sharing and help to manage risks associated with sharing large volumes of sensitive data. Following the code and adopting its practical recommendations will help to give organisations confidence to collect and share personal data in a way that is fair, transparent where appropriate and in line with the rights and expectations of the people whose information is being shared.

The code will help organisations to identify what they need to consider before sharing personal data, and clarify when it is appropriate to share. Key considerations around data sharing include the following:

- Having a clear objective or set of objectives for the data sharing.
- It can be harmful not to share data; what are the risks of not sharing the data?
- Is the planned data sharing necessary and proportionate?
- Fairness and transparency.
- What is the lawful basis for sharing the data? Only sharing the minimum amount of data needed to achieve the objectives: could it be anonymised or pseudonymised instead?
- The risks of detriment that the data sharing poses to individuals, especially to vulnerable individuals.
- Compliance with individuals' rights under data protection legislation.
- Ensuring accountability: this includes data protection by design and default, and documenting all data sharing operations.
- Robust safeguards around the entire data sharing process, including restricting access to the data, ensuring accuracy, setting retention periods and putting security measures in place.
- A data sharing agreement will help organisations to meet their data protection obligations.
- Where data sharing is planned on a 'regular' basis, as is suggested in this consultation, the data sharing agreement will set out the detailed arrangements and processes.

Data controllers will need to take into account which data protection regime the processing falls under (GDPR or DPA 2018) and to ensure that the appropriate lawful basis for processing is outlined and documented taking into consideration whether they are processing special category data.

Attention should also be drawn to the fact that the processing of personal data must always be fair as well as lawful and should not have unjustified, adverse effects on individuals. The potential that the processing may have a detrimental impact on individuals also needs to be factored. Processing should generally not occur in a way that an individual would not reasonably expect and it needs to be justified in all circumstances.

Any data sharing initiatives should be in accordance with the aims and objectives set out in the Serious Violence Strategy. It is also important to define more specifically who is captured by the statement 'those most at risk of becoming *affected* by serious violence' and to differentiate between different categories of individuals impacted. Our experience has shown that issues may arise where distinctions are not made between the categories of individuals captured by the processing and this can have unjustified adverse effects, this is explored in further detail below under the 'Gangs Matrix' heading.

Q.9 Do you consider that Option One would best achieve the consultation vision? Please explain why.

The Information Commissioner does not propose to provide a preferred option to achieve the consultation vision, but seeks to provide a view relating to the necessary data protection considerations under each option.

It is important to note that there are **already** provisions in data protection legislation which allow for the sharing of personal data. This questions the requirement for a further separate legislative duty. Any new legal requirements introduced will need to be consistent with those set out in the data protection legislation, and that they accord with the good practice that will be set out in the forthcoming Data Sharing Code of Practice. Additionally, careful scrutiny will be needed to ensure that they do not duplicate what already exists in data protection law, which would run the risk of legislative confusion.

Data protection is sometimes wrongly cited as a barrier to data sharing. Instead, data protection law should be viewed as a framework of safeguards to ensure fair, lawful and proportionate data sharing. We have discussed the data protection legislation and the Data Sharing Code of Practice in our response to Question 8.

It is recognised though that there are a number of other legislative requirements that apply to the specified authorities listed in Annex A. The introduction of new primary legislation may consolidate these to promote consistency in the sharing of data and intelligence. Furthermore, the sharing of personal data, particularly special category data in certain sectors can be problematic due to the potential conflicts with common law duties of confidentiality. This issue could be addressed through a statutory approach.

If a legal requirement is introduced, we would expect that, at the policy making stage, safeguards should be applied in order to ensure that the processing is fair and proportionate. Any unforeseen detriment or negative consequences which may arise in relation to the individuals whose data is shared should be considered, particularly in relation to vulnerable individuals and children. When processing children's data, due regard should be taken of the safeguards and necessary requirements. This would minimise the risks for practitioners when sharing data once the legislation has come into effect. At both the drafting stage, and in practice, the relationship with data protection law should be clear.

The Information Commissioner welcomes the statement that the government intends to publish guidance to help specified agencies to comply with the new duty and recommends that due regard to the data protection requirements and to the Data Sharing Code of Practice is paid in this guidance. The Information Commissioner would be willing to engage on the data protection and data sharing elements of this guidance. The development and dissemination of guidance is a key measure, and would support organisations in their data sharing activity.

Furthermore, it is essential that individual organisations understand their obligations as controllers and set up appropriate governance measures to support their staff. Our experience shows that breaches are more likely to occur when staff have received inadequate training and good practice hasn't been embedded. Whilst there are examples of good practice in relation to data sharing, our investigations have shown the negative impacts on individual lives when things go wrong when effective governance arrangements are not put in place.

Q. 11 Do you consider that Option two would best achieve the consultation vision? Please explain why.

Should a decision be made to legislate in order to commit organisations to becoming members of Community Safety Partnerships, consideration is required as to the controller relationship between the Specified Authority and the partnerships. This includes whether the organisations are

considered as joint controllers and whether the Community Safety Partnerships are controllers in their own right. In this instance, the Partnerships may be required to pay the data protection fee to the Information Commissioner's Office. Joint controllers must consider who will take primary responsibility for complying with the data protection obligations, in particular transparency obligations and individuals' rights. In short, each party must have a clear understanding of where their responsibilities start and end, data sharing agreements will assist with this. Joint controllers will have to agree an arrangement under article 26 of the GDPR where they set out these terms.

If there is a need for data sharing, it will be essential to comply with data protection legislation; the forthcoming Data Sharing Code will provide practical guidance as to how to do this. We discussed this topic in our response to Question 8.

Q.13 Do you consider that Option three would best achieve the consultation vision? Please explain why.

It is important to reinforce the fact that data protection should not be viewed as a barrier to data sharing; rather, the data protection legislation provides a framework to conduct data sharing fairly and proportionately. This will be supported by the forthcoming Data Sharing Code of Practice. If a non-statutory approach is taken, robust governance arrangements are necessary to ensure that the data protection obligations are adhered to. Any guidance produced should draw attention to the Data Sharing Code of Practice and the Information Commissioner's Office would be willing to engage on this where appropriate.

If this option is chosen, it would be advisable to consider Article 40 of the GDPR which provides for relevant bodies to draw up codes of conduct which would help their sector ensure data protection compliance and reflect the specific needs of the relevant controllers and help them to work together. The Information Commissioner would be willing to engage with the relevant bodies if a decision is taken to produce a code of conduct to offer advice. Further information on codes of conduct can be found on our website.

Gangs Matrix Enforcement Notice

It is relevant to draw attention to this recent investigation by the Information Commissioner as it highlights the importance of effective governance. The Metropolitan Police Service's (MPS) Gangs Matrix consisted of a database which recorded intelligence related to alleged gang members and victims of gang related crimes. This investigation resulted in an enforcement notice being issued to the MPS in November 2018 requiring

the MPS to take specified steps to comply with the Data Protection Principles set out in the terms of the notice. Whilst it was determined that the aim of the data sharing between the police, local authorities and education authorities to counter gang culture was a valid public interest to pursue, key issues needed to be addressed. The recommendations include taking steps to improve guidance, distinguishing between victims and offenders, complying with retention periods, ensuring information shared with partner agencies is done so securely and proportionately and conducting a DPIA.

Public Health Approach

The consultation also makes reference to the 'public health' approach to preventing and tackling serious crime to understand the causes and consequences of serious violence. Data Protection requirements therefore need to be followed to ensure that the processing is fair and that the relevant considerations in relation to any profiling are taken into account.

Comparisons can be drawn to the ICO investigation into the public health model of reducing violence which followed the investigation into the Gangs Matrix. The investigation outcome found that the Violence Reduction models examined demonstrated measurable reductions in violence. Each approach used anonymised, pseudonymised or minimal personal data sets to inform strategic decisions about where the resources of various public services should be directed. The benefits are that the use of anonymised or pseudonymised data sets reduces the risks of this approach to individuals' privacy rights.

Information Commissioner

24 May 2019